

Docket No. 213422US2S/btm



2161

#d

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Taku KATO, et al.

GAU: 2161

SERIAL NO: 09/941,687

EXAMINER:

FILED: August 30, 2001

FOR: RECORDING METHOD, PRODUCING METHOD, PLAYBACK METHOD, APPARATUS, AND
INFORMATION RECORDING MEDIUM

REQUEST FOR PRIORITY

RECEIVED

OCT 23 2001

Group 2100

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:


<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2000-260903	August 30, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
 - ☐ are submitted herewith
 - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


Marvin J. Spivak

Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26,803



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 8月30日

出 願 番 号

Application Number:

特願2000-260903

出 願 人

Applicant(s):

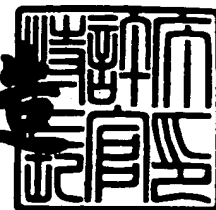
株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 8月24日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3076352

【書類名】 特許願

【整理番号】 A000005280

【提出日】 平成12年 8月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/14

【発明の名称】 記録方法、再生方法、装置及び情報記録媒体

【請求項の数】 7

【発明者】

 【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中事業所内

 【氏名】 加藤 拓

【発明者】

 【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中事業所内

 【氏名】 遠藤 直樹

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

 【識別番号】 100068814

 【弁理士】

 【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 記録方法、再生方法、装置及び情報記録媒体

【特許請求の範囲】

【請求項 1】 所定の鍵管理情報が記録された第 1 の読取専用領域と、前記鍵管理情報が所定の関数で圧縮されてなる圧縮データが前記第 1 の読取専用領域とは異なる記録方式で記録された第 2 の読取専用領域と、暗号化コンテンツデータを書換え可能に記録するための書換え可能領域とを備えた情報記録媒体に情報を記録するための記録方法であって、

前記情報記録媒体の第 1 の読取専用領域から鍵管理情報を読み出し、この鍵管理情報を所定の関数を用いて圧縮データに変換する圧縮ステップと、

前記情報記録媒体の第 2 の読取専用領域から圧縮された鍵管理情報を読み出し、前記圧縮ステップで得られた圧縮データと比較する比較ステップと、

前記比較ステップで両者が一致したとき、自己の保有するデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する鍵生成ステップと、

入力されたコンテンツデータを前記鍵生成ステップで生成したコンテンツ鍵を用いて暗号化し、得られた暗号化コンテンツデータを前記書換え可能領域に記録する暗号化記録ステップと、

を含んでいることを特徴とする記録方法。

【請求項 2】 所定の鍵管理情報が記録された第 1 の読取専用領域と、前記鍵管理情報が所定の関数で圧縮されてなる圧縮データが前記第 1 の読取専用領域とは異なる記録方式で記録された第 2 の読取専用領域と、暗号化コンテンツデータを書換え可能に記録するための書換え可能領域とを備えた情報記録媒体から情報を再生するための再生方法であって、

前記情報記録媒体の第 1 の読取専用領域から鍵管理情報を読み出し、この鍵管理情報を所定の関数を用いて圧縮データに変換する圧縮ステップと、

前記情報記録媒体の第 2 の読取専用領域から圧縮された鍵管理情報を読み出し、前記圧縮ステップで得られた圧縮データと比較する比較ステップと、

前記比較ステップで両者が一致したとき、自己の保有するデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する鍵生成ステップと、

前記情報記録媒体の書換え可能領域から前記暗号化コンテンツデータを読み出し、この暗号化コンテンツデータを前記鍵生成ステップで生成したコンテンツ鍵を用いて復号し、得られたコンテンツデータを出力する復号ステップと、
を含んでいることを特徴とする再生方法。

【請求項 3】 所定の鍵管理情報が記録された第 1 の読取専用領域と、前記鍵管理情報が所定の関数で圧縮されてなる圧縮データが前記第 1 の読取専用領域とは異なる記録方式で記録された第 2 の読取専用領域と、暗号化コンテンツデータを書換え可能に記録するための書換え可能領域とを備えた情報記録媒体に情報を記録するための記録装置であって、

前記情報記録媒体の第 1 の読取専用領域から鍵管理情報を読み出し、この鍵管理情報を所定の関数を用いて圧縮データに変換する圧縮手段と、

前記情報記録媒体の第 2 の読取専用領域から圧縮された鍵管理情報を読み出し、前記圧縮手段で得られた圧縮データと比較する比較手段と、

前記比較手段で両者が一致したとき、自己の保有するデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する鍵生成手段と、

入力されたコンテンツデータを前記鍵生成手段で生成したコンテンツ鍵を用いて暗号化し、得られた暗号化コンテンツデータを前記書換え可能領域に記録する暗号化記録手段と、

を備えたことを特徴とする記録装置。

【請求項 4】 所定の鍵管理情報が記録された第 1 の読取専用領域と、前記鍵管理情報が所定の関数で圧縮されてなる圧縮データが前記第 1 の読取専用領域とは異なる記録方式で記録された第 2 の読取専用領域と、暗号化コンテンツデータを書換え可能に記録するための書換え可能領域とを備えた情報記録媒体から情報を再生するための再生装置であって、

前記情報記録媒体の第 1 の読取専用領域から鍵管理情報を読み出し、この鍵管理情報を所定の関数を用いて圧縮データに変換する圧縮手段と、

前記情報記録媒体の第 2 の読取専用領域から圧縮された鍵管理情報を読み出し、前記圧縮手段で得られた圧縮データと比較する比較ステップと、

前記比較手段で両者が一致したとき、自己の保有するデバイス鍵を用いて、鍵

管理情報からコンテンツ鍵を生成する鍵生成手段と、

前記情報記録媒体の書換え可能領域から前記暗号化コンテンツデータを読み出し、この暗号化コンテンツデータを前記鍵生成手段で生成したコンテンツ鍵を用いて復号し、得られたコンテンツデータを出力する復号手段と、

を備えたことを特徴とする再生装置。

【請求項 5】 所定の鍵管理情報が記録された第 1 の読取専用領域と、

前記鍵管理情報が所定の関数で圧縮されてなる圧縮データが前記第 1 の読取専用領域とは異なる記録方式で記録された第 2 の読取専用領域と、

暗号化コンテンツデータを書換え可能に記録するための書換え可能領域と、
を備えており、

前記鍵管理情報は、読み出された後に所定の関数により圧縮データに変換されて前記第 2 の読取り専用領域内の圧縮データと比較されるためのデータであり、

前記暗号化コンテンツデータは、この比較結果が一致したときに記録可能となる記録対象データであることを特徴とする情報記録媒体。

【請求項 6】 所定の鍵管理情報及び暗号化コンテンツデータを書換え可能に記録するための書換え可能領域と、前記鍵管理情報が所定の関数で圧縮されてなる圧縮データが前記第 1 の読取専用領域とは異なる記録方式で記録された第 2 の読取専用領域とを備えた情報記録媒体に情報を記録するための記録方法であって、

前記情報記録媒体の書換え可能から鍵管理情報を読み出し、この鍵管理情報を所定の関数を用いて圧縮データに変換する圧縮ステップと、

前記情報記録媒体の第 2 の読取専用領域から圧縮された鍵管理情報を読み出し、前記圧縮ステップで得られた圧縮データと比較する比較ステップと、

前記比較ステップで両者が一致したとき、自己の保有するデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する鍵生成ステップと、

入力されたコンテンツデータを前記鍵生成ステップで生成したコンテンツ鍵を用いて暗号化し、得られた暗号化コンテンツデータを前記書換え可能領域に記録する暗号化記録ステップと、

を含んでいることを特徴とする記録方法。

【請求項 7】 所定の鍵管理情報及び暗号化コンテンツデータを書換え可能に記録するための書換え可能領域と、前記鍵管理情報が所定の関数で圧縮される圧縮データが前記第 1 の読取専用領域とは異なる記録方式で記録された第 2 の読取専用領域とを備えた情報記録媒体から情報を再生するための再生方法であって、

前記情報記録媒体の書換え可能領域から鍵管理情報を読み出し、この鍵管理情報を所定の関数を用いて圧縮データに変換する圧縮ステップと、

前記情報記録媒体の第 2 の読取専用領域から圧縮された鍵管理情報を読み出し、前記圧縮ステップで得られた圧縮データと比較する比較ステップと、

前記比較ステップで両者が一致したとき、自己の保有するデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する鍵生成ステップと、

前記情報記録媒体の書換え可能領域から前記暗号化コンテンツデータを読み出し、この暗号化コンテンツデータを前記鍵生成ステップで生成したコンテンツ鍵を用いて復号し、得られたコンテンツデータを出力する復号ステップと、

を含んでいることを特徴とする再生方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、鍵情報あるいは鍵管理情報の記録された記録方法、再生方法、装置及び情報記録媒体に関する。

【0002】

【従来の技術】

コンテンツデータ等の記録される情報記録媒体では、鍵情報や鍵管理情報はその情報が不正に書換えられてしまうことを防ぐために、通常は読取専用領域に記録されるが、それらのデータサイズが読取専用領域サイズを越えてしまうことがある。

【0003】

【発明が解決しようとする課題】

以上説明したように従来の情報記録媒体では、不正な書換えを防ぐ観点から、

鍵情報や鍵管理情報を読取専用領域に記録すると、それらのデータサイズが読取専用領域サイズを越えてしまうことがある。

【0004】

本発明は上記実情を考慮してなされたもので、DVD-RAM等のような読取専用領域のサイズが限られている記録媒体において、鍵情報や鍵管理情報が不正に書換えられることを防ぐ記録方法、再生方法、装置及び情報記録媒体を提供することを目的とする。

【0005】

【課題を解決するための手段】

本発明の骨子は、鍵情報や鍵管理情報を書換え可能領域に記録すると共に、それらの情報をハッシュ関数等の圧縮関数を用いて圧縮し、その圧縮されたデータを読取専用領域に記録することによって、鍵情報や鍵管理情報の不正書換えや不正コピーの検出を可能にすることにある。

【0006】

また、書換え可能領域に記録された鍵情報や鍵管理情報を利用する際には、それらの情報を読み出して適切な圧縮関数によって圧縮した結果と読取専用領域に予め記録されている圧縮情報の一致を確認することによって、鍵情報や鍵管理情報の正当性を検証する。

【0007】

さて以上のような本発明の骨子に基づいて具体的には以下のような手段が講じられる。

【0008】

第1の発明は、所定の鍵管理情報が記録された第1の読取専用領域と、前記鍵管理情報が所定の関数で圧縮されてなる圧縮データが前記第1の読取専用領域とは異なる記録方式で記録された第2の読取専用領域と、暗号化コンテンツデータを書換え可能に記録するための書換え可能領域とを備えた情報記録媒体が用いられる。

【0009】

第1の発明では、情報記録媒体に情報を記録するための記録方法や記録装置と

して、前記情報記録媒体の第 1 の読取専用領域から鍵管理情報を読み出し、この鍵管理情報を所定の関数を用いて圧縮データに変換する圧縮ステップと、前記情報記録媒体の第 2 の読取専用領域から圧縮された鍵管理情報を読み出し、前記圧縮ステップで得られた圧縮データと比較する比較ステップと、前記比較ステップで両者が一致したとき、自己の保有するデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する鍵生成ステップと、入力されたコンテンツデータを前記鍵生成ステップで生成したコンテンツ鍵を用いて暗号化し、得られた暗号化コンテンツデータを前記書換え可能領域に記録する暗号化記録ステップとを含んでもよい。

【0010】

また、第 1 の発明では、情報記録媒体から情報を再生するための再生方法や再生装置として、前記情報記録媒体の第 1 の読取専用領域から鍵管理情報を読み出し、この鍵管理情報を所定の関数を用いて圧縮データに変換する圧縮ステップと、前記情報記録媒体の第 2 の読取専用領域から圧縮された鍵管理情報を読み出し、前記圧縮ステップで得られた圧縮データと比較する比較ステップと、前記比較ステップで両者が一致したとき、自己の保有するデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する鍵生成ステップと、前記情報記録媒体の書換え可能領域から前記暗号化コンテンツデータを読み出し、この暗号化コンテンツデータを前記鍵生成ステップで生成したコンテンツ鍵を用いて復号し、得られたコンテンツデータを出力する復号ステップとを含んでもよい。

【0011】

次に、第 2 の発明は、所定の鍵管理情報及び暗号化コンテンツデータを書換え可能に記録するための書換え可能領域と、前記鍵管理情報が所定の関数で圧縮されてなる圧縮データが前記第 1 の読取専用領域とは異なる記録方式で記録された第 2 の読取専用領域とを備えた情報記録媒体が用いられる。

【0012】

第 2 の発明では、情報記録媒体に情報を記録するための記録方法及び記録装置として、前記情報記録媒体の書換え可能から鍵管理情報を読み出し、この鍵管理情報を所定の関数を用いて圧縮データに変換する圧縮ステップと、前記情報記録媒体の第 2 の読取専用領域から圧縮された鍵管理情報を読み出し、前記圧縮ステップ

で得られた圧縮データと比較する比較ステップと、前記比較ステップで両者が一致したとき、自己の保有するデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する鍵生成ステップと、入力されたコンテンツデータを前記鍵生成ステップで生成したコンテンツ鍵を用いて暗号化し、得られた暗号化コンテンツデータを前記書換え可能領域に記録する暗号化記録ステップとを含んでいてもよい。

【 0 0 1 3 】

また、第2の発明は、情報記録媒体から情報を再生するための再生方法及び再生装置として、前記情報記録媒体の書換え可能領域から鍵管理情報を読み出し、この鍵管理情報を所定の関数を用いて圧縮データに変換する圧縮ステップと、前記情報記録媒体の第2の読取専用領域から圧縮された鍵管理情報を読み出し、前記圧縮ステップで得られた圧縮データと比較する比較ステップと、前記比較ステップで両者が一致したとき、自己の保有するデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する鍵生成ステップと、前記情報記録媒体の書換え可能領域から前記暗号化コンテンツデータを読み出し、この暗号化コンテンツデータを前記鍵生成ステップで生成したコンテンツ鍵を用いて復号し、得られたコンテンツデータを出力する復号ステップとを含んでいてもよい。

【 0 0 1 4 】

(作用)

本発明によれば、読取専用領域のサイズが限られた記録媒体においても、不正書換えや不正コピーを防止した上で大量の鍵情報や鍵管理情報を記録することができる。

【 0 0 1 5 】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施形態を説明する。

【 0 0 1 6 】

本実施形態では、記録媒体として書換え可能領域、読取専用領域および他の領域とは製造時の書込み方法が異なる読取専用領域を持った記録媒体（記録用DVDディスク）を例にとって説明する。

【 0 0 1 7 】

(第 1 の実施形態)

以下、第 1 の実施形態について説明する。

【 0 0 1 8 】

図 1 は、本実施形態において記録用 DVD ディスク作製時にディスクに記録される情報と各々の情報が書込まれる領域を図示している。ディスク作成者は予め定められた鍵管理情報を書換え可能領域（領域 1）に記録すると共に、読取専用領域（領域 2）に当該鍵管理情報を予め定められた関数によって圧縮したデータを記録する。

【 0 0 1 9 】

図 2 は、本実施形態においてユーザ所有の記録機器によって著作権付きコンテンツを記録する方法を示しており、その手順を以下の各ステップに示す。

【 0 0 2 0 】

1) 記録機器は、ディスクの書換え可能領域（領域 1）に記録されている鍵管理情報を読み出し、その情報を予め定められた圧縮関数を用いて圧縮する。

【 0 0 2 1 】

2) 記録機器は、ディスクの読取専用領域（領域 2）に記録されている圧縮された鍵管理情報を読み出し、Step 1 で計算した圧縮データと比較する。比較結果が異なっていた場合は、本記録処理を終了する。

【 0 0 2 2 】

3) 記録機器は、自身に予め与えられているデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する。

【 0 0 2 3 】

4) 記録機器は、Step 3 で求められたコンテンツ鍵を用いて機器に入力されたコンテンツデータを暗号化し、暗号化されたコンテンツをディスクの書換え可能領域（領域 1）に記録する。

【 0 0 2 4 】

次に、上記手順によってディスク上に記録された著作権付きコンテンツを再生する手段を図 3 に基づいて以下の各ステップに示す。

【 0 0 2 5 】

1) 再生機器は、ディスクの書換え可能領域（領域1）に記録されている鍵管理情報を読み出し、その情報を予め定められた圧縮関数を用いて圧縮する。

【0026】

2) 再生機器は、ディスクの読取専用領域（領域2）に記録されている圧縮された鍵管理情報を読み出し、Step 1で計算した圧縮データと比較する。比較結果が異なっていた場合は、本記録処理を終了する。

【0027】

3) 再生機器は、自身に予め与えられているデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する。

【0028】

4) 再生機器は、ディスク上の書換え可能領域（領域1）に記録されている暗号化コンテンツを読み出し、Step 3で求められたコンテンツ鍵を用いて暗号化コンテンツを復号して、所定の方法でコンテンツデータを出力する。

【0029】

なお、上記記録機器と再生機器が異なる場合だけでなく、同じ機器であることもある。

【0030】

本実施形態においては、鍵管理情報自体は書換え可能領域に書込まれているため、ユーザは鍵管理情報を削除したり書換えたりすることが可能であるが、削除／書換えを行った場合には著作権付きコンテンツを正しく記録／再生できなくなってしまうため、鍵管理情報の不正な削除／書換えはユーザの不利益となる。但し、不可抗力によって嗅ぎ管理情報を削除してしまった場合などに対応するために、ディスク製造者はインターネット上のWeb-Siteなどで鍵管理情報を公開しておき、ユーザが自由に鍵管理情報の修復ができるようにしておくことも考えらる。

【0031】

（第2の実施形態）

以下、第2の実施形態について説明する。

【0032】

図4は、本実施形態において記録用DVDディスク作製時にディスクに記録される情報と各々の情報が書込まれる領域を図示している。ディスク作成者は予め定められた鍵管理情報を読取専用領域（領域2）に記録すると共に、領域2とは記録方法の異なる読取専用領域（領域3）に当該鍵管理情報を予め定められた関数によって圧縮したデータを記録する。

【0033】

ここで、領域3は、例えば、DVD-R、DVD-RW、DVD-RAMのBurst Cutting Areaに対応する領域である。

【0034】

この領域3は、他の領域1や領域2とは異なった方法で書込まれており、読み出す際には読み出し装置が領域1や領域2とは完全に区別して読出すことができる領域である。

【0035】

ここで、領域2は、不正なユーザが製造途中に領域2に記録されていないDiscを入手し、ユーザの書込装置を改造などして不正書込を行なうことが比較的容易にできる領域である。

【0036】

これに対して、領域3は、ユーザの書込装置に実装されていない手段によって書込される領域であり、不正な書込が非常に困難な領域である。

【0037】

しかし、領域3への書込作業が大変であるため、鍵管理情報をこの領域に書込むことは実際には実現困難であり、その圧縮データのみを記録するのである。

【0038】

なお、これらの鍵管理情報や圧縮データはディスク作成者が用意する以外に、所定のライセンス組織からライセンスされる形態も考えられる。

【0039】

図5は本実施形態においてユーザ所有の記録機器によって著作権付きコンテンツを記録する方法を示しており、その手順を以下の各ステップに示す。

【0040】

1) 記録機器は、ディスクの読取専用領域（領域 2）に記録されている鍵管理情報を読み出し、その情報を予め定められた圧縮関数を用いて圧縮する。

【0 0 4 1】

2) 記録機器は、ディスクの記録方法が特別な読取専用領域（領域 3）に記録されている圧縮された鍵管理情報を読み出し、Step 1 で計算した圧縮データと比較する。比較結果が異なっていた場合は、本記録処理を終了する。

【0 0 4 2】

3) 記録機器は、自身に予め与えられているデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する。

【0 0 4 3】

4) 記録機器は、Step 3 で求められたコンテンツ鍵を用いて機器に入力されたコンテンツデータを暗号化し、暗号化されたコンテンツをディスクの書換え可能領域（領域 1）に記録する。

【0 0 4 4】

次に、上記手順によってディスク上に記録された著作権付きコンテンツを再生する手段を図 6 に基づいて以下の各ステップに示す。

【0 0 4 5】

1) 再生機器は、ディスクの読取専用領域（領域 2）に記録されている鍵管理情報を読み出し、その情報を予め定められた圧縮関数を用いて圧縮する。

【0 0 4 6】

2) 再生機器は、ディスクの記録方法が特別な読取専用領域（領域 3）に記録されている圧縮された鍵管理情報を読み出し、Step 1 で計算した圧縮データと比較する。比較結果が異なっていた場合は、本記録処理を終了する。

【0 0 4 7】

3) 再生機器は、自身に予め与えられているデバイス鍵を用いて、鍵管理情報からコンテンツ鍵を生成する。

【0 0 4 8】

4) 再生機器は、ディスク上の書換え可能領域（領域 1）に記録されている暗号化コンテンツを読み出し、Step 3 で求められたコンテンツ鍵を用いて暗号化コ

ンテンツを復号して、所定の方法でコンテンツデータを出力する。

【0049】

なお、上記記録機器と再生機器が異なる場合だけでなく、同じ機器であることもある。また、SDカード、ICカード等でも、その場合はSDカードのコントローラが読み取り、書込可能を制御する。また、第2の実施形態では、Burst Cutting Areaの代わりに、ROMを別途設けることにより実現できる。

【0050】

なお、上記実施形態に記載した記録・再生技術は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピーディスク、ハードディスクなど）、光ディスク（CD-ROM、DVDなど）、光磁気ディスク（MO）、半導体メモリなどのプログラムを記憶でき（記憶形式は何れの形態であっても良い）、かつコンピュータが読み取り可能な記憶媒体に格納して頒布することもできる。

【0051】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【0052】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【0053】

また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【0054】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づ

き、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【0055】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0056】

なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わされた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【0057】

その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【0058】

【発明の効果】

以上説明したように本発明によれば、以上詳記したように本発明によれば、鍵情報や鍵管理情報のサイズを暗号学的に安全な圧縮関数などによって圧縮したデータを読取専用領域に安全に記録することによって、サイズの大きい元の鍵情報や鍵管理情報を保護することが可能となる。

【図面の簡単な説明】

【図1】

本発明の第1の実施形態に係る記録媒体の情報記録領域を示す図

【図2】

同実施形態における記録媒体に著作権付きコンテンツを記録する手順を示す図

【図 3】

同実施形態における記録媒体から著作権付きコンテンツを読み出す手順を示す

図

【図 4】

本発明の第 2 の実施形態に係る記録媒体の情報記録領域を示す図

【図 5】

同実施形態における記録媒体に著作権付きコンテンツを記録する手順を示す図

【図 6】

同実施形態における記録媒体から著作権付きコンテンツを読み出す手順を示す

図

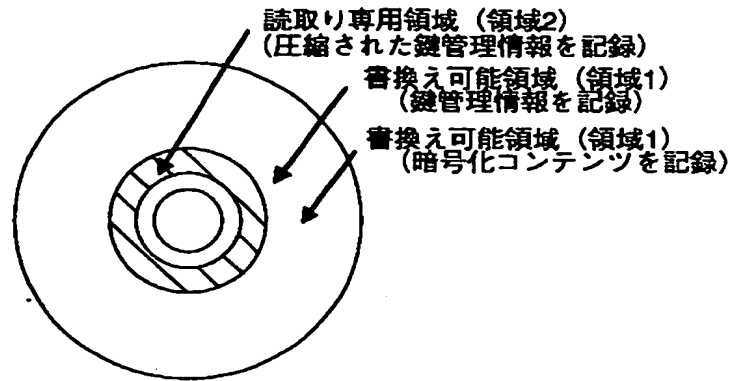
【符号の説明】

1 ～ 3 … 領域

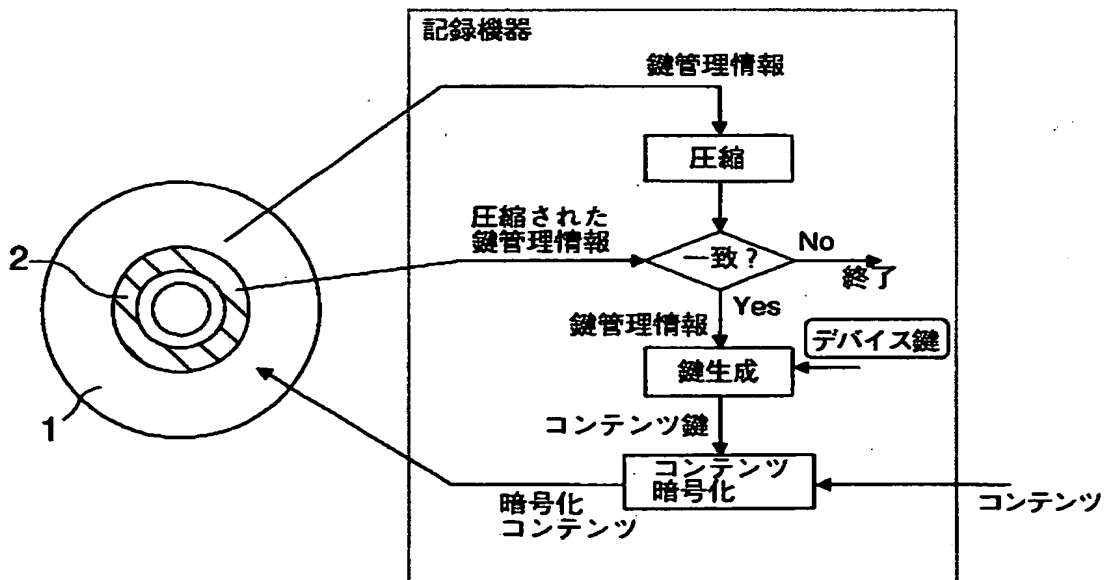
【書類名】

図面

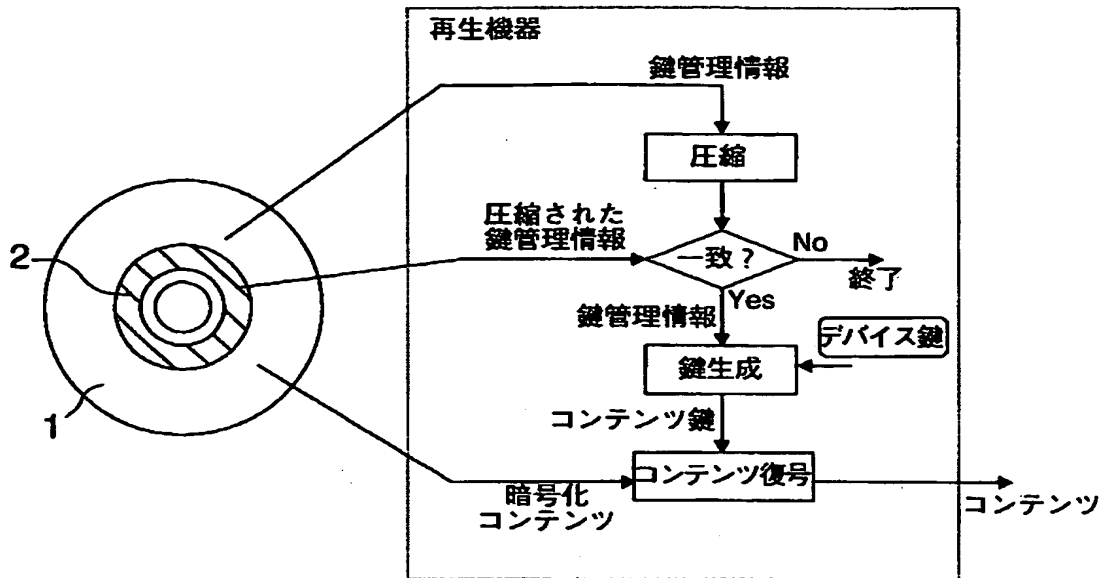
【図1】



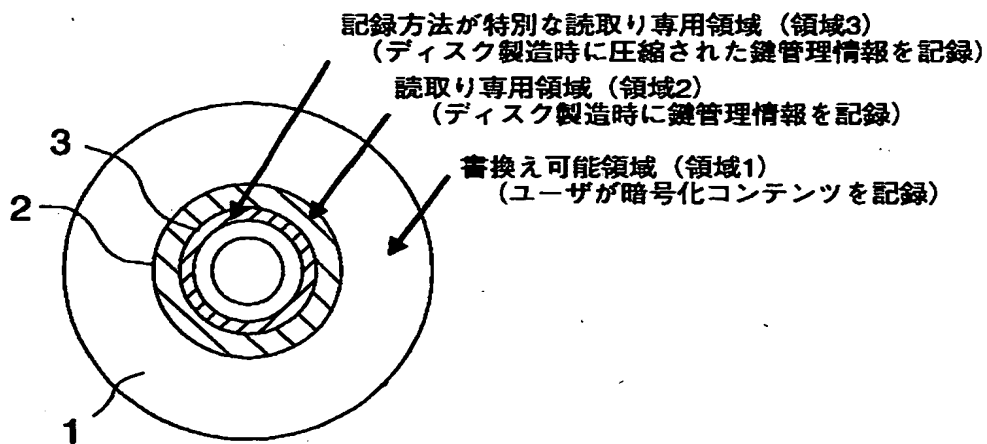
【図2】



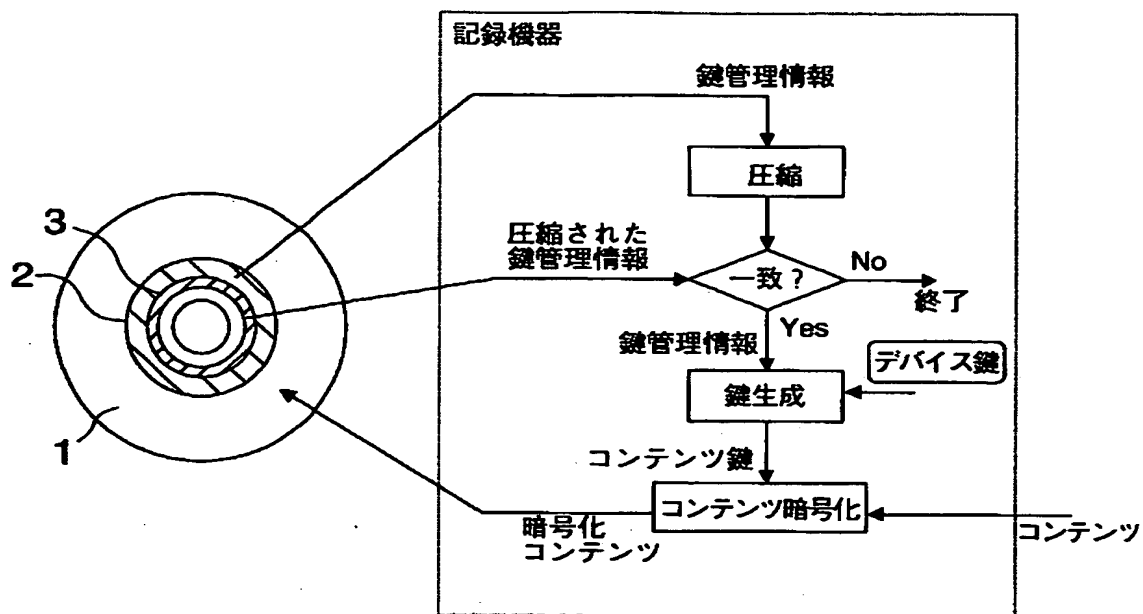
【図3】



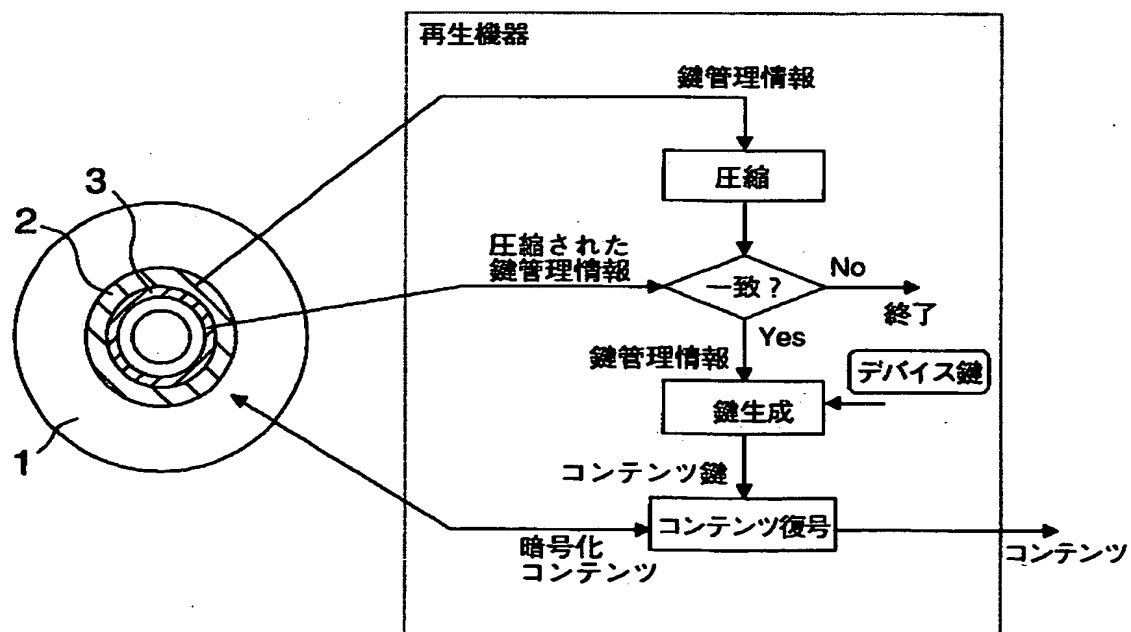
【図4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 鍵情報や鍵管理情報を圧縮したデータをより小さな読取専用領域に記録することによって鍵情報や鍵管理情報の保護を可能にする。

【解決手段】 鍵情報や鍵管理情報のサイズを暗号学的に安全な圧縮関数などによって圧縮したデータを読取専用領域に安全に記録することによって、サイズの大きい元の鍵情報や鍵管理情報を保護する手段を備える。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日 1990年 8月22日
[変更理由] 新規登録
住 所 神奈川県川崎市幸区堀川町72番地
氏 名 株式会社東芝
2. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝